CHAPTER

3 Compliance with Standards, Regulations, and Laws

Information security governance has been characterized as the fourth wave of security management. The first wave was technical in nature, the second wave was managerial, the third wave was institutional, and the fourth wave is about governance. All persons concerned with information security, from the board of directors, to the chief executives, to information technology and information security professionals, and employees of the organization must be concerned with information security governance.

The typical driver of information security governance is the prevention of financial fraud through the manipulation of an organization's electronic data. Attempts to prevent abuse and fraud have led to increased regulations, standards, and guidelines, causing organizations to pay greater attention to governance, which has changed the dynamics of information security management. Computer crimes and cyber attacks are on the rise, many of which are perpetrated by the use of social engineering techniques. Building security awareness into the governance structure has become essential.

Information security professionals are faced with ever-evolving technologies, sophisticated and determined cyber criminals, a blended threat landscape, and increased compliance requirements based on new corporate governance initiatives. Even those security practitioners who work in nonregulated environments are expected to follow a common set of practices, criteria, and standards. An understanding of the laws, regulations, and standards that apply to the field of information security is essential. Fortunately, there are substantial overlaps among the best practices commonly accepted by these, and this chapter covers those.

Information Security Standards

Also known as voluntary standards, or perhaps frameworks, these sets of "best practices" have been developed and published by internationally recognized organizations, and accepted by the information security profession in general. The most well-known of these are

- Control Objectives for Information and related Technology (COBIT)
- International Organization for Standardization (ISO) 27001 and 27002
- National Institute of Standards and Technology (NIST) standards

COBIT

COBIT is published by ISACA, the Information Systems Audit and Control Association. ISACA is a widely recognized independent IT governance organization, and its COBIT guidelines are used by IT management in many organizations to define and manage processes based on a maturity model like the Capability Maturity Model (CMM). COBIT is not about information security—it is a general IT standard, but certain security practices are embedded within it. COBIT contains a higher-level set of information security guidelines than the ISO 27000 series, intended to align business goals with IT goals.

ISACA periodically updates the COBIT processes and releases new versions. COBIT 4.1 is organized around four conceptual areas, referred to as domains, corresponding to the preferred order an organization would use to roll out security program components along the lines of the well-known Plan, Do, Check, Adjust (PDCA) growth cycle commonly used to build and continuously improve services. COBIT 5 expands on these four domains and adds a fifth domain for Governance. The domains in versions 4 and 5 are as follows.

Governance:

- (v5) Evaluate, Direct, and Monitor (EDM)

Management:

- (v4.1) Plan and Organize (PO) and (v5) Align, Plan, and Organize (APO)
- (v4.1) Acquire and Implement (AI) and (v5) Build, Acquire, and Implement (BAI)
- (v4.1) Deliver and Support (DS) and (v5) Deliver, Service, and Support (DSS)
- (v4.1) Monitor and Evaluate (ME) and (v5) Monitor, Evaluate, and Assess (MEA)

Key information security–related components of COBIT 4 (which are carried forward into version 5) include

- **PO2.3** Establish an information classification scheme based on the criticality and confidentiality of data, and include ownership information, protection, retention, and destruction requirements.
- **PO4.8** Establish an IT security and risk management function at a senior level of an organization's management.
- **PO6, PO7.4** Implement a security awareness program along with formal security training for employees, service providers, and third parties.
- **PO9** Perform risk assessment and management via a risk management program that analyzes and communicates risks and their potential impact on business processes.
- **PO10.12** Ensure that security requirements are embedded into the project management process.
- **AI2.4** Include security requirements in the application development process to ensure security and availability in line with the organization's objectives.

- **AI3.2, AI3.3** Implement security in the configuration, integration, and maintenance of hardware and software to provide availability and integrity.
- **AI5.2** Ensure that third-party suppliers of IT infrastructure, facilities, hardware, software, and services comply with the organization's security requirements, and this is reflected in any contracts with those third parties.
- **AI7.1–AI7.9** Follow a well-defined change control process that includes testing, production migration, and backout planning.
- **DS1.3, DS2.2** Include security requirements in Service Level Agreements (SLAs).
- **DS4.1–DS4.10** Perform Business Continuity Planning (BCP) with periodic testing, and ensure that backups are preserved in a safe offsite location.
- **DS5.1–DS5.11** Manage security according to a specific plan, perform identity management and user account management, perform security testing and monitoring, perform incident detection and response, implement security protections, employ cryptographic key management, protect against malicious software, secure the network, and protect data exchanges.
- **DS12.1–DS12.5** Control physical security and access to important assets with access controls, escorts, and monitoring of activities.

ISO 27000 Series

The ISO 27000 series of information security standards provides a set of frameworks for developing a security program from concept to maturity. It's broken up into several parts in order to be manageable—each part prescribes a set of activities that belong to phases comparable to those in the Plan-Do-Check-Act (or more accurately, Plan-Do-Check-Adjust) (PDCA) cycle, similar to what COBIT does.

- **ISO 27001** is a high-level specification for the management of an information security program. This is referred to as an information security management system (ISMS). The ISO 27001 standard contains high-level statements about management responsibilities such as defining objectives, measuring performance, and auditing compliance. It contains provisions to begin with a risk assessment to determine which controls are the most important for each organization, and how fully they should be applied. In principle, this is somewhat similar to COBIT's "Plan and Organize" concept or the "Plan" part of the PDCA cycle. It is possible to be audited against this standard (voluntarily, for organizations that aspire to a high level of maturity).
- **ISO 27002** is a detailed set of information security controls that would ideally be driven by the output of the risk assessment performed as part of ISO 27001. This standard forms a complete reference to all the things an organization might want to do. It can be viewed as a set of best practices, and it's up to each organization to determine which of them apply to their business environment. This can be viewed as somewhat similar to COBIT's "Acquire and Implement" concept or the "Do" part of the PDCA cycle.

- **ISO 27003** is intended to provide recommendations and best practices to implement the ISMS management controls defined by ISO 27001—in other words, how to deliver the security program. This can be compared to the "Deliver and Support" concept of COBIT, or the "Check" part of the PDCA cycle.
- **ISO 27004** covers measurement of the effectiveness of the ISMS implemented by the first three ISO 27000 standards, using metrics and key performance indicators to describe how well the information security controls are operating. This can be thought of in the context of COBIT's "Monitor and Evaluate" concept, or the "Adjust" part of the PDCA cycle.
- **ISO 27005** defines a risk management framework for information security that can be used to inform the decisions within ISO 27001 that lead to selection of controls for ISO 27002.
- **ISO 27006** is a standard that provides guidelines for professional organizations that provide certification to be properly accredited.

The ISO 27000 series framework combines the familiar initial risk assessment with controls essential for compliance with typical regulations plus controls considered to be common best practices for information security. Best practice controls include the creation of an information security policy document, development of an organizational plan with clearly defined security responsibilities, security education and training, proper incident reporting, and development of a disaster-recovery plan.

Consider the following list of topical domains from ISO 27002, to get an idea of the type of coverage provided by the standard (sections 0 through 3 are introductory material, and section 4 defines the risk management approach that should be used to determine which controls in the remaining 12 sections are relevant to each organization):

- **Risk Assessment and Treatment** The use of risk assessment as a basis for selecting appropriate security controls.
- **Security Policy** The clear expression of management intent for information protection.
- **Organization of Information Security** Defining and staffing the roles and functions needed by the security program.
- **Asset Management** The responsibility and classification of assets, including data.
- **Human Resources Security** Ensuring that the behaviors of trusted inside employees don't defeat the security controls, because the majority of security problems come from insiders, not outsiders.
- **Physical and Environmental Security** Creating secure areas and protecting equipment.
- **Communications and Operations Management** Maintaining a safe, reliable, and correct IT environment (including the parts outside the direct control of the organization, provided by third parties). Malware protection, backups, and network security are included here.
- **Access Control** User controls and responsibilities, including access controls for the networks, operating systems, and applications, along with mobile computing.

- **Information Systems Acquisition, Development, and Maintenance** Security requirements, ensuring integrity and confidentiality, change management in development and support processes, and vulnerability management.
- **Information Security Incident Management** Reporting security issues and vulnerabilities, and managing incidents.
- **Business Continuity Management** Information security aspects of business continuity.
- **Compliance** Legal requirements, compliance with policies, standards, and specifications, and audit considerations.

Some important examples from ISO 27002 that would likely be of interest to most organizations include

- **4.1, 4.2** Establish a formal risk management program to assess and treat risks to the organization's assets.
- **5.1** Publish an information security policy that reflects senior management's expectations with regard to security, and make sure it is available to all stakeholders.
- **6.1** Establish an internal security organization with appropriate, well-defined responsibilities and relationships with third parties.
- **6.2** Use confidentiality agreements to protect information when working with third parties, to protect access to confidential information.
- **7.1** Identify and document assets, assign ownership, classify according to criticality, and establish an acceptable use policy.
- **7.2** Establish an information classification scheme that includes labeling and handling guidance.
- **8.1–8.3** Perform background checks on employment candidates, communicate security responsibilities to all employees, provide information security awareness and training, and ensure that the correct security behaviors are enforced through a disciplinary process.
- **9.1, 9.2** Establish physical security controls, including perimeters, access controls, separation of critical areas, and protection of equipment.
- **10.1** Establish a change control process along with separation of duties to separate development and production environments and activities.
- **10.2** Manage third-party service delivery.
- **10.3** Perform capacity planning and resource monitoring for proactive allocation of resources.
- **10.4** Protect against malware.
- **10.5** Establish reliable backups.
- **10.6** Establish network security controls.
- **10.7** Manage the handling and disposal of data and the media it resides on, and transport data securely so it can't be intercepted.

- **10.9** Protect online systems, data, and transactions and maintain accurate audit logs to identify issues.
- **11.2–11.6** Manage user access rights to control access to data.
- **12.2** Make sure that applications are correctly processing information and that they check their inputs to avoid misuse, and use encryption to protect that information.
- **12.5** Manage source code development and access, and use a formal change control process to promote code from development into the production environment.
- **12.6** Establish a vulnerability management program.
- **13.1, 13.2** Establish an incident response program.
- **14.1** Perform business continuity management, including regular testing.
- **15.1–15.3** Establish a compliance management program to comply with all legal and regulatory requirements. Perform audits to ensure compliance.

NIST

The National Institute of Standards and Technology (NIST) provides a set of "Special Publications" to assist industry, government, and academic organizations with following best practices. Known as the "800 series," the set of security-specific publications is very specific to individual technologies, with the exception of 800-53.

800-53 was developed primarily for the U.S. Federal Government, to specify security control organization and structure, security control baselines, common controls, security controls in external environments, security control assurance, risk management, information system categorization, security control selection, and monitoring of security controls.

800-53 is organized into 18 "security control families," which are conceptual categories that represent important components of a complete security program.

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Security Assessment and Authorization
5. Configuration Management
6. Contingency Planning
7. Identification and Authentication
8. Incident Response
9. Maintenance
10. Media Protection
11. Physical and Environmental Protection
12. Planning

13. Personnel Security
14. Risk Assessment
15. System and Services Acquisition
16. System and Communications Protection
17. System and Information Integrity
18. Program Management

Each remaining 800 series publication provides guidance on specific subject areas, and they are constantly updated as technologies emerge and change. The NIST web site is the best place to look for technology-specific documents. Some examples of technology standards that can be found there include

- SP 800-153: Guidelines for Securing Wireless Local Area Networks (WLANs)
- SP 800-147: BIOS Protection Guidelines
- SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing
- SP 800-133: Recommendation for Cryptographic Key Generation
- SP 800-128: Guide for Security-Focused Configuration Management of Information Systems
- SP 800-124: Guidelines on Cell Phone and PDA Security
- SP 800-123: Guide to General Server Security
- SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- SP 800-121: Guide to Bluetooth Security
- SP 800-119: Guidelines for the Secure Deployment of IPv6
- SP 800-118: Guide to Enterprise Password Management
- SP 800-115: Technical Guide to Information Security Testing and Assessment
- SP 800-114: User's Guide to Securing External Devices for Telework and Remote Access
- SP 800-113: Guide to SSL VPNs
- SP 800-111: Guide to Storage Encryption Technologies for End User Devices
- SP 800-101: Guidelines on Cell Phone Forensics
- SP 800-100: Information Security Handbook: A Guide for Managers
- SP 800-98: Guidelines for Securing Radio Frequency Identification (RFID) Systems
- SP 800-95: Guide to Secure Web Services
- SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)
- SP 800-92: Guide to Computer Security Log Management
- SP 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

- SP 800-83: Guide to Malware Incident Prevention and Handling
- SP 800-77: Guide to IPsec VPNs
- SP 800-72: Guidelines on PDA Forensics
- SP 800-69: Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist
- SP 800-68: Guide to Securing Microsoft Windows XP Systems for IT Professionals
- SP 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- SP 800-64: Security Considerations in the System Development Life Cycle
- SP 800-63: Electronic Authentication Guideline
- SP 800-58: Security Considerations for Voice Over IP Systems
- SP 800-55: Performance Measurement Guide for Information Security
- SP 800-50: Building an Information Technology Security Awareness and Training Program
- SP 800-45: Guidelines on Electronic Mail Security
- SP 800-44: Guidelines on Securing Public Web Servers
- SP 800-41: Guidelines on Firewalls and Firewall Policy
- SP 800-40: Creating a Patch and Vulnerability Management Program
- SP 800-30: Guide for Conducting Risk Assessments
- SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
- SP 800-12: An Introduction to Computer Security: The NIST Handbook

Regulations Affecting Information Security Professionals

There are many government regulations that apply to various organizations. These regulations are different from the standards described in the previous section because they are required, instead of being aspirational. But regulations and standards are not mutually exclusive. There is a lot of overlap between the standards described in the previous section and the regulations included in this section. In many cases, it may make sense for the security practitioner to strive for compliance with both a regulation and a standard (such as HIPAA and ISO 27000, for example).

Sector-specific regulations that affect information security professionals who work in certain organizations include the following:

- **Gramm-Leach-Bliley Act (GLBA)** Applies to the financial sector, including banks and lenders, for the protection of customer and financial information
- **Sarbanes-Oxley Act of 2002, Section 404 (SOX 404 or Sarbox)** Applies to all publicly traded companies to guarantee data integrity against financial fraud

- **Health Insurance Portability and Accountability Act (HIPAA) and companion HITECH Act** Applies to the healthcare sector, regarding the protection of patient information
- **North American Electric Reliability Corporation Critical Infrastructure Protection reliability standards (NERC CIP)** Applies to electric service providers such as utility companies, solar and wind power generators, and nuclear power generators
- **Payment Card Industry (PCI) Data Security Standard (DSS)** Applies to any organization that processes, transmits, or stores credit card information

The Duty of Care

Recognizing the categories of network behavior that constitute criminal acts enables information security professionals to take the offensive effectively upon discovery of such conduct. Increasingly, however, chief information officers (CIOs) are focused on the legal issues surrounding their organization's defensive posture. Specifically, CIOs are growing more concerned about liability arising from their organizations' efforts to achieve one of the information security staff's core functions: safeguarding the security of the organization's information. Information security regulation, and the concomitant prospect of incurring liability for falling short of industry standards for preparing for, preventing, and responding to security breaches, is a key driver for information technology strategy.

This proliferation of federal and state regulations has largely been aimed at protecting electronically stored, personally identifiable information, and the regulations have generally been confined in their application to certain industry sectors. The regulations establish a basis for liability and accountability for entities that fail to apply the requisite safeguards. Although most of the regulations enacted to date are sector-specific, the combination of the regulations and the forthcoming proposals is generating significant momentum toward recognition of a long elusive "industry standard" for information security.

The first prominent regulation began with the industry-specific safeguards for financial institutions required by the Gramm-Leach-Bliley Act. The protections of these safeguards have been gradually expanded to the health-care industry by the Health Insurance Portability and Accountability Act, and to nonregulated industries through consent decrees entered in connection with enforcement actions brought by both the Federal Trade Commission and state attorneys general. In addition, California has recently enacted its own non-sector-specific reporting requirements for information security breaches. The cumulative effect of these developments is an emerging duty of care for any entity that obtains or maintains personally identifiable information electronically, and one that may logically be expected to extend to the government and to corporate America's general information security posture. A discussion of the existing regulations provides some shape and contour to the measures that organizations should now consider essential to secure their systems.

Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act of 1999 (GLBA) was enacted to reform the banking industry, and among its methods was the establishment of standards for financial institution safeguarding of non-public personal information. Each federal agency with authority over financial institutions was charged with establishing standards to ensure the security and

confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

Each implementing agency took a slightly different tack. Individual financial agencies, such as the Federal Reserve System and the Federal Deposit Insurance Corporation, acted first, developing interagency banking guidelines in 2001 applying specifically to the institutions under their jurisdictions. The Federal Trade Commission Safeguards Rule, which became effective in May of 2003, is perhaps the most significant because it applies broadly to any financial institution not subject to the jurisdiction of another agency that collects or receives customer information. The defining element of the Safeguards Rule is the requirement that each financial institution "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue."[1]

The Rule sets forth five specific elements that must be contained in an entity's information security program:

- Designate an employee or employees to coordinate the information security program to ensure accountability
- Assess risks to customer information in each area of its operations, especially employee training and management, information systems, and attack or intrusion response
- Design and implement safeguards to control the assessed risks, and monitor the effectiveness of the safeguards
- Select service providers that can maintain appropriate safeguards, and include safeguard requirements in service provider contracts
- Evaluate and adjust the information security program based on the results of effectiveness monitoring and on material changes to the organization

15 U.S.C. Section 6801(b)(1)–(3)

The agencies responsible for establishing these safeguard standards are the Federal Trade Commission (FTC); the Office of the Comptroller of the Currency (OCC); the Board of Governors of the Federal Reserve System (Board); the Federal Deposit Insurance Corporation (FDIC); the Office of Thrift Supervision (OTS); the National Credit Union Administration (NCUA); the Secretary of the Treasury (Treasury); and the Securities and Exchange Commission (SEC). The NCUA, the OCC, the Board, the FDIC, and the OTS have issued final guidelines that are even more rigorous than the FTC Safeguards Rule discussed here. The SEC also adopted a final Safeguards Rule as part of its Privacy of Consumer Financial Information Final Rule. (See 17 C.F.R. part 248.)

[1] 16 C.F.R. part 314.

The interagency banking guidelines implementing GLBA provide some additional specifics with regard to practical application of safeguards. While they outline risk assessment in the same manner as the FTC Safeguards Rule—entities should identify potential threats, then assess the likelihood of occurrence and the sufficiency of security measures designed to meet those threats—they provide more detailed suggestions for risk management. For instance, the banking guidelines suggest several methods for restricting access to customer information, thereby reducing vulnerability. Among these suggested methods are the following:

- Restrict data access only to authorized individuals
- Prevent authorized individuals from providing the information to unauthorized individuals
- Restrict access to the physical locations that contain customer information
- Encrypt electronic customer information
- Restrict access of customer information to employees who are prescreened using background checks
- Implement dual control procedures that require two or more persons, operating together, to access information

While the interagency banking guidelines apply only to financial institutions under the jurisdiction of the promulgating agencies, their guidelines for risk management serve as a useful reference for all entities that collect or receive customer information.

Finally, the Securities and Exchange Commission released its own Regulation S-P in 2001. Regulation S-P requires every broker-dealer, fund, and registered adviser to adopt policies and procedures to address the safeguards. Consistent with safeguards promulgated by other agencies, Regulation S-P requires that the adopted policies and procedures be reasonably designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the information, and protect against unauthorized access that could result in substantial customer harm or inconvenience. Unlike many of the other agencies, however, the SEC opted not to mandate any particular attributes that should be included in the policies, nor did it provide specific guidelines for ensuring the regulation's goals were met.

Although each agency took a slightly different approach, when viewed as a whole, it is clear that certain common attributes permeate all of the various agency implementations of the Gramm-Leach-Bliley safeguards—namely that the information security requirements placed on a particular organization should be commensurate with the risks facing that organization, and that written response plans and reporting mechanisms are essential to addressing those risks. Each agency recognized that the duty to safeguard personal information through risk assessment and risk management is directly proportional to the potential vulnerability of the information and to the quantity and quality of the information to be protected. For this reason, both the FTC Safeguards Rule and the interagency banking guidelines are centered on the performance of an initial vulnerability assessment, followed by the implementation of policies and procedures tailored to address the potential risk of compromised customer information.

Sarbanes-Oxley Act

Although the SEC's implementing regulations for GLBA were the least rigorous of any agency, information security oversight by that agency may nonetheless emerge as a serious issue under the purview of the more general Sarbanes-Oxley Act of 2002. The SEC placed additional restrictions on public companies as a result of the Sarbanes-Oxley Act, which requires in section 404 that the annual reports of covered entities contain an "internal control report." This report must indicate management's responsibility for establishing and maintaining adequate internal controls for the purpose of financial reporting, and must contain an assessment of the effectiveness of those controls.[2] Signed into law in the wake of the Enron and WorldCom scandals, Sarbanes-Oxley imposes substantial criminal penalties on officers responsible for failure to accurately report.

The SEC states that registrants must implement "policies and procedures that … [p]rovide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements."[3] The Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and Office of Thrift Supervision issued a joint policy in March 2003 that characterizes "internal controls" as a process designed to provide reasonable assurances that companies achieve the following internal control objectives: efficient and effective operations, including safeguarding of assets; reliable financial reporting; and, compliance with applicable laws and regulations. Among the core management process components identified in the policy are risk assessment and monitoring activities, both key attributes of information security procedures.[4] Although neither the SEC rule nor the joint agency guidance single out information security as a component of "internal controls" reporting, the increasing significance of information security issues to large organizations, coupled with the requirements of officer and board of director oversight of information security in sector-specific regulation, puts information security squarely onto the Sarbanes-Oxley checklists for major corporations.

HIPAA Privacy and Security Rules

Much as the Gramm-Leach-Bliley Act sought to regulate the protection of personal information in the financial industry, the Health Insurance Portability and Accountability Act (HIPAA) introduced standards for the protection of health-related personal information. Passed in 1996, HIPAA required the Department of Health and Human Services to issue Privacy and Security Rules for the protection of individually identifiable

[2] *Sarbanes-Oxley Act of 2002*, Section 404.

[3] See *Final Rule: Management's Report on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports*, Release No. 34-47986 (June 5, 2003), 68 Fed. Reg. 36,636 (June 18, 2003) available at www.sec.gov/rules/final/33-8238.htm.

[4] See *Interagency Policy Statement on the Internal Audit Function and Its Outsourcing* (March 17, 2003) (updating the FDIC's and other federal banking agencies' guidance on the independence of an accountant who provides both external and internal audit services to an institution as a result of the auditor independence provisions of the Sarbanes-Oxley Act of 2002) available at www.federalreserve.gov/boarddocs/press/bcreg/2003/20030317/attachment.pdf; Internal Audits, FIL-21-2003 (March 17, 2003) available at www.fdic.gov/news/news/financial/2003/fil0321.html.

health information maintained electronically by health plans, health-care clearinghouses, and certain health-care providers.

The Privacy Rule contains a general information security provision requiring covered entities to implement "appropriate administrative, technical and physical safeguards" for the protection of personal health information. The Security Rule imposes more specific standards on covered entities. In practice, compliance with the standards of the Security Rule is the measure for evaluating "appropriate safeguards" under the Privacy Rule. Accordingly, the Security Rule safeguards are the relevant standards that regulated agencies should incorporate into their information security plans.

Like the financial industry safeguards, the HIPAA Security Rule requires covered entities to first perform a risk assessment and then adopt security measures commensurate with the potential risk. The Rule sets out four general requirements:

- Ensure the confidentiality, integrity, and availability of all electronic personal information created, received, maintained, or transmitted by the entity
- Protect against any reasonably anticipated threats or hazards to the information
- Protect against information disclosure prohibited by the Privacy Rule
- Ensure compliance with the Rule by its workforce

Before developing security measures designed to meet these requirements, the entity must first perform an individualized assessment that considers the size of the entity and its infrastructure and security capabilities, the cost of security measures, and the potential likelihood and scope of threats to personal information. The breadth of these considerations suggests that several groups within an organization—IT, information security, legal, risk managers, human resources—may all need to be included in conducting the initial assessment. In other words, a routine prepackaged penetration test or the equivalent from a computer security vendor is unlikely to achieve the specific goals of the assessment.

Once the risk assessment has been completed, the organization must then adopt administrative, physical, and technical safeguards that are defined with a greater level of specificity in the HIPAA Rule than previous information security regulations. The Security Rule's specific standards include both "required" and "addressable" implementation specifications. Where a specification is "addressable" and not required, the covered entity must assess whether it is a "reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic personally identifiable health information." The entity must implement the specification if reasonable and appropriate; however, if doing so is not reasonable and appropriate, the entity must document its reasons for this conclusion and implement an "equivalent alternative measure."

The required safeguards include a number of familiar concepts included in the GLBA safeguards, as well as more specific, yet still technology-neutral requirements. For example, the administrative safeguards require the implementation of a security management process that includes written policies and procedures to prevent, detect, contain, and correct security violations. The policies must include a risk analysis, risk management, and employee sanction policy, an emergency contingency plan, and address information access management. Entities are also required to conduct security awareness training in support

of these policies. Physical safeguards include facility access controls, workstation security, and media controls. Technical safeguards require access control and authentication but leave the use of encryption of transmitted data and automatic logoff access controls as "addressable" rather than "required" safeguards. Finally, the HIPAA Security Rule requires that covered entities ensure by written contract that business associates will protect information transmitted by the entity. Because a business associate essentially must agree to comply with the Security Rule's requirements with respect to any electronic protected health information (ePHI) that it creates, receives, maintains, or transmits on behalf of the covered entity, this requirement effectively extends the application of the HIPAA Security Rule beyond the specific regulated sector to all entities sharing data with it.

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) is part of the American Recovery and Reinvestment Act of 2009 (ARRA) and a massive expansion of the HIPAA Security and Privacy Rules in regard to the exchange of ePHI. HITECH changes the following HIPAA sections:

- Enforcement
- Notification of Breach
- Electronic Health Record Access
- Business Associates and Business Associate Agreements

Enforcement penalties will be imposed for "willful neglect" and can range from $250,000 to $1.5 million with repeat/uncorrected violations. Breach notification laws require mandatory reporting for any unauthorized exposure of unencrypted ePHI. Individuals, upon request, may receive an electronic copy of their health records. Business associates are now directly responsible, just as covered entities are, for the security and privacy of ePHI.

Thus, the HIPAA Security Rule, like the Gramm-Leach-Bliley safeguards, focuses largely on initial and updated evaluations of vulnerability, followed by steps for developing an information security plan, leaving flexibility on specifics so that the plan can be tailored to the organization and the risk.

NERC CIP

NERC, the North American Electric Reliability Corporation, publishes a "cyber security framework" known as Critical Infrastructure Protection (CIP). The main purpose of this set of requirements is to ensure continued operation of the power grid, especially in the event of a terrorist attack or other sabotage.

The main focus of NERC CIP is on what NERC refers to as Critical Cyber Assets, which are any components (usually considered to be technology and computing devices) that are necessary to the continued, reliable operation of electric power generation. Thus, the goal of NERC CIP is to protect Critical Cyber Assets that support reliable operation of the power grid, which NERC refers to as the Bulk Electric System.

The first step in this framework is to identify (and document) the Critical Cyber Assets through a risk-based assessment. The framework provides a specific approach to that identification and risk assessment, based on assigning criticality and vulnerability attributes to the Critical Cyber Assets along with identification of risks that those assets may be exposed to.

After the assets are identified and categorized, the framework requires "minimum security management controls" that should be employed to protect against the identified risks. These controls include

- Physical access is expected to be restricted to authorized people who have appropriate security training and awareness, and their access should be limited only to those areas to which they require access to perform their job functions. A security perimeter must be defined, and physical security controls are placed within that perimeter.
- Security management of systems identified as Critical Cyber Assets must include methods, processes, and procedures for security. These also apply to noncritical assets inside the security perimeter (sharing the same network as the critical assets).
- The identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets must be reported to the appropriate systems, governmental agencies, and regulatory bodies.
- Business continuity planning (BCP) and disaster recovery (DR) plans must be in place and functionally effective.

NERC publishes these standards, and the plans needed to comply with them, as a free download at www.nerc.com/docs/standards/rs/Reliability_Standards_Complete_Set.pdf.

PCI DSS: Payment Card Industry Data Security Standard

Developed in 2004 by several organizations that provide credit services, especially focused on credit card numbers (CCNs), this standard applies to a large number of organizations because so many organizations accept credit cards for payments. It is intended primarily to protect the security of "cardholder data"—namely cardholder name, account number, expiration date, service code, magnetic stripe or chip data, verification code, and PIN numbers. Theft of these data elements costs credit organizations enormous amounts of money, typically due to fraudulent use of credit card numbers by thieves, and PCI DSS is an attempt to put reasonable protections in place to reduce that theft, and its associated costs.

Despite being focused on data specific to credit card transactions, PCI DSS looks quite similar to more general security frameworks. It has 12 provisions, organized into 6 general categories, as follows. If you compare these to the other standards in this chapter, such as ISO 27002, you'll see the similarity.

Build and Maintain a Secure Network:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data:

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program:

5. Use and regularly update antivirus software or programs
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures:

7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks:

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy:

12. Maintain a policy that addresses information security for all personnel

Laws Affecting Information Security Professionals

Information security professionals, along with the technology solutions they choose to deploy, form the primary line of defense against incursions into government and corporate computer networks. As the first responders to network incidents, particularly those emanating from outside the organization, these professionals are responsible for evaluating when network events rise above the normal background noise. In order to assess those events meaningfully, it is imperative that information security professionals have some understanding of the laws that govern misconduct on networks.

Knowledge of the elements of the various computer crimes defined by federal statutes, as well as those included in state statutes, is vital to information security professionals. This is not only because it assists information security professionals in defending their organizations' data, products, and communications from outside threats, but because it enables them to reduce their organizations' liability for actions taken by their own employees. Unwanted network activity takes on a variety of forms and occurs along a continuum that runs from mere bothersome nuisances to potentially terminable employment offenses to federal felonies.

Understanding the basic elements of computer crimes has several advantages:

- It informs the decision of whether to elevate notice of certain conduct to others within the organization. When the information security staff knows the key attributes that form criminal conduct, they are far less likely to sound alarms in response to non-actionable events.
- It enables information security professionals to position their organizations to make sound criminal referrals (or to build solid civil cases). Computer crime laws are somewhat unique in that they impose a large degree of responsibility on the victim

for taking steps to establish the commission of a cyber crime, including defining access permissions and documenting damage. Awareness of this responsibility enables information security professionals to design their network defense posture and to collect and document critical evidence when responding to incidents. In most cases, information security managers will take a lead role in drafting their organizations' information security policies, and recognition of the key computer crime elements can be incorporated into those policies.

- It will assist in preventing overly aggressive actions in response to incidents that might subject a system administrator to liability.

Computer crimes can generally be divided into three categories: the "hacking" laws, which cover intrusions into computer networks and subsequent fraud, theft, or damage; the "electronic communications" laws, which govern the interception, retrieval, and disclosure of e-mail and keystrokes; and other "substantive" laws, which address otherwise unlawful conduct either committed in cyberspace or assisted by computers.

Legislation for all information security professionals in the United States, regardless of the type of organization they work for, includes

- The Computer Fraud and Abuse Act
- The USA PATRIOT Act
- The Electronic Communications Privacy Act (ECPA)
- The Economic Espionage Act
- State-specific information security law
- Other criminal and civil law relating to theft and abuse
- Regulated industry-specific requirements
- Law enforcement requirements

The following sections describe some of the important aspects of these legal provisions that information security professionals should be aware of.

Hacking Laws

The laws covering network intrusions that result in fraud, theft, or damage are referred to as the "hacking" laws. The most prominent of these are the Computer Fraud and Abuse Act, and parts of the USA PATRIOT Act. The specific relevance of these laws to information security professionals are as follows.

The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA), codified at 18 U.S.C. Section 1030, is the seminal law on computer crimes. Designed to protect the confidentiality, integrity, and availability of data and systems, the CFAA targets attackers and others who access or attempt to access computers without authorization and inflict some measure of damage. Such prohibited access includes not only direct hacking into a system, but also denial of service attacks, viruses, logic bombs, ping floods, and other threats to information security.

Two key sets of concepts permeate the CFAA:

- Access without or in excess of authorization
- Damage or loss

With rare exception, these two elements must be met to establish a CFAA crime. Because these concepts are central to all violations, it's important to understand their meaning in the context of the statute.

For the purpose of the CFAA, the "access without authorization" prong actually can take two distinct forms. The first is a straight "unauthorized access," which is defined in terms of a traditional trespass—an outsider without privileges or permission to a certain network breaks into that network. For traditional unauthorized access, the intent of the trespasser is irrelevant.

In addition to straight trespass, the CFAA also relies on the concept of gaining access to a computer system in "excess of authorization." Recognizing when a user has exceeded his or her level of authorization can be a far more subtle determination than identifying a straight unauthorized access. "Excess of authorization" can be established both by reference to the purpose of the perpetrator's access and the extent of the access. By way of example, an authorized user on an organization's network may have rights subject to limitations on the scope of access—the user is not permitted to have system administrator privileges or to access certain shared drives that are dedicated to storing sensitive information. If that user, while authorized to be on the network, elevates his privileges to root access, or somehow gains access to the restricted shared drive, she is transformed from an authorized user to one acting "in excess of authorization." Similarly, the same user may also be given access to information on the network but only for a specific purpose—an IRS agent may access taxpayer files, but only for those taxpayers on whose cases the agent is working. If that agent begins browsing taxpayer files unrelated to her job function, the *improper purpose* for which she is accessing the information may transform the otherwise authorized use into an "excess of authorization." Defining an act as purely unauthorized, as opposed to exceeding authorization, can be significant, as certain sections of the CFAA require proof that the perpetrator's access was wholly unauthorized, while mere "excess of authorization" is sufficient for others.

NOTE Indeed, the First Circuit Court of Appeals recognized that an IRS employee's browsing of taxpayer information out of idle curiosity, where such activity was forbidden by IRS employment policy, constituted access in excess of authorization. *U.S. v Czubinski*, 106 F.3d 1069, 1078-79 (1st Cir. 1997). By contrast, a violation does not exist where a defendant can establish that the reason for the access was approved. See *Edge v Professional Claims Bureau*, Inc., 64 F.Supp.2d 116, 119 (E.D.N.Y. 1999) (granting summary judgment to defendant who accessed a credit report for a permissible purpose).

The second set of key concepts in the CFAA is "damage" or "loss." The CFAA defines damage as "*any* impairment to the integrity or availability of data, a program, system, or information."

Each section of the CFAA incorporates these concepts of unauthorized access plus damage in defining the specific conduct prohibited by that section. When evaluating whether

"Damage" Is Defined by Section 1030(a)(5)(B)

For certain provisions of the CFAA, damage is confined to the following subset of specific harms:

- Loss to one or more persons affecting one or more protected computers aggregating to at least $5,000
- Any modification or potential modification to the medical diagnosis, treatment, or care of one or more individuals
- Physical injury to any person
- A threat to public health or safety
- Damage affecting a computer system used by government for administration of justice, national defense, or national security

unwanted network activity constitutes a crime, the threshold issue should be isolating the unauthorized access. Upon that determination, the next question an information security manager should ask is "What 'plus' factor exists?" Mere trespass (of a nongovernment computer) alone does not constitute a crime under federal law. Accordingly, there must be some additional activity that causes damage or loss in some form in order to constitute a crime. The nature of that "something more" varies by section of the CFAA, as is demonstrated by the following review of the most regularly charged 1030 offenses.

Section 1030(a)(2) has perhaps the broadest application of any section, as it protects the confidentiality of data, irrespective of whether any damage is caused to the integrity or availability of the data. 1030(a)(2) prohibits intentionally accessing a computer without or in excess of authorization and thereby obtaining information in a financial record or a credit report, from a federal agency, or from a "protected computer" if conduct involved an interstate or foreign communication. In essence, 1030(a)(2) reaches both forms of unauthorized access, and the only requisite "plus factor" is obtaining information.[5] This provision has been further broadened by courts holding that the mere viewing of information during a period of unauthorized access constitutes "obtaining" the information, even if it is not copied, downloaded, or otherwise converted.[6] In recognition of its having the least egregious "plus factor," violations of 1030(a)(2) are misdemeanors, not felonies (meaning they carry a maximum sentence of one year in prison), unless they are committed for commercial advantage or private financial gain, for criminal or tortious purposes, or if the value of information exceeds $5,000.

[5] *America Online, Inc. v LCGM, Inc.*, 46 F.Supp.2d 444 (E.D. Va. 1998) (defendant who maintained an AOL membership for the purpose of harvesting e-mail addresses of AOL members in violation of AOL's Terms of Service exceeded authorized access, which combined with demonstrable loss by plaintiff established violation of Section 1030(a)(2)).

[6] See, for example, *Shurgard Storage Ctrs., Inc. v Safeguard Self Storage, Inc.*, 119 F.Supp.2d 1121 (W.D.Wash. 2000).

Section 1030(a)(4) criminalizes either form of unauthorized access in connection with a scheme to defraud. Specifically, this section prohibits "knowingly and with the intent to defraud, accessing a protected computer without or in excess of authorization, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value." Here, the "plus factors" are the existence of a fraudulent scheme in connection with the hack, as well as the acquisition of something of value. The CFAA specifically excludes the theft of small-scale computer time (less than $5,000 in one year) as the potential thing of value. Accordingly, "hacks for access" where the victim's computer resources are the only thing taken (such as leveraging the wireless network of a neighboring company) do not constitute an (a)(4) violation, despite the presence of an unauthorized access coupled with an intent to defraud (unless a loss of over $5,000 can be demonstrated). 1030(a)(4) violations are felonies carrying a five year maximum sentence and $250,000 maximum fine for first time offenses.

Section 1030(a)(5) covers the classic computer hacking violations—intentional release of worms and viruses, denial of service attacks, and computer intrusions that damage systems. The section is broken into three distinct parts. First, Section 1030(a)(5)(A)(i) prohibits knowingly causing the transmission of a "program, information, code, or command" and, as a result of such conduct, intentionally causing "damage" without authorization to a protected computer. This subsection has a strict *intent* element—the wrongdoer must knowingly commit the act while intending to cause damage—but it is unique among CFAA crimes in that it applies to either insiders or outsiders as it does not require any level of unauthorized access. Section (a)(5)(A)(i) crimes are those where no level of access is necessarily required to commit the offense, as in a SYN flood attack, where an outsider manages to knock a system offline without ever gaining access.

NOTE In the case of *United States v Morris*, 928 F.2d 504 (2nd Cir. 1991), a defendant who released a worm into national networks connecting university, governmental, and military computers around the country was found guilty of accessing federal interest computers without authorization under former Section 1030(a)(5)(A). The Morris worm, considered by many to be the first malware outbreak, is mentioned further in Chapter 31.

Section 1030(a)(5)(A)(ii) and (iii) govern traditional computer hacking by outsiders that causes damage to the victim system. Section (a)(5)(A)(ii) prohibits intentionally accessing a protected computer without authorization and *recklessly* causing damage; Section (a)(5)(A)(iii) criminalizes the same unlawful access coupled with causing any damage, negligently or otherwise. The severity of the penalties depends on whether the damage was caused recklessly (a felony) or negligently (a misdemeanor). Thus, unlike (a)(5)(A)(i), the latter two subsections do require an "unauthorized access" coupled with the causing of damage. Significantly, both (a)(5)(A)(ii) and (iii) require that the perpetrator be an "outsider," as someone merely exceeding authorized access cannot commit either offense. For all three subsections of 1030(a)(5), the conduct must result in the previously identified subsets of "damage" set forth in 1030(a)(5)(B). Accordingly, bothersome and potentially nefarious conduct, such as repeated port-scanning, where no actual unauthorized access has occurred and no actual damage has resulted, do not reach the level of a 1030(a)(5) violation.[7]

[7] *Moulton v VC3*, 2000 WL 33310901 (N.D. Ga. 2000).

USA PATRIOT Act (Sections 808, 814, 816)

The USA PATRIOT Act contains several provisions that apply to computer security, notably the following:

Section 808 adds certain computer fraud and abuse offenses to the list of violations that may constitute a federal crime of terrorism. The new provisions apply to: anyone who knowingly accesses a computer without authorization and obtains classified information; and, anyone who knowingly causes the transmission of a program, information, code, or command, and as a result intentionally causes damage to a protected computer. The inclusion of these offenses in the definition of a federal crime of terrorism in Section 2332b(g)(5)(B) relates primarily to who has investigatory authority over the offenses (the Attorney General, in this case). However, by virtue of cross references in other parts of the Act, including these offenses in the definition of terrorism also affects: the extension of their statute of limitations (Section 809 of the Act); post-release supervision of someone convicted of these offenses under certain circumstances (Section 812 of the Act); and, applicability of the racketeering statutes (Section 813 of the Act). According to Section 809, should these computer offenses result in or create a foreseeable risk of death or serious bodily injury, there is no statute of limitations. Under similar conditions, Section 812 could lead to life-time post-release supervision. The cross-reference to racketeering statutes gives law enforcement officials more tools with which to prosecute computer trespassers.

Section 814 increases the penalties for certain computer fraud and abuse offenses. The penalty for a first offense of causing the transmission of a program, information, code or command that intentionally causes damage to a protected computer increases from 5 years to 10 years. The penalty for a second such offense or a second offense of intentionally gaining unauthorized access to a protected computer and, as a result, recklessly causing damage is increased from 10 years to 20 years. Also, it is now an offense to attempt to commit these offenses even if the attempt is not successful or does not cause any damage. This section also redefines "damage." Damage is now defined as: i) loss to one or more persons during any 1-year period aggregating at least $5,000 in value; ii) modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals; iii) physical injury to any person; iv) a threat to public health or safety; v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security. Prior to this, it was not clear whether the $5,000 threshold was per person affected or the total value of damages caused to all people affected. The new language clarifies that it is the latter. Finally, the Section also modifies the language in 18 U.S.C. 1030 regarding civil suits. This includes new language that says victims suffering damages resulting from an offense listed in section 1030 may not sue under this section for negligent design or manufacture of hardware, software, or firmware. This is a broad immunity that protects manufacturers should any design or manufacture problem lead to damages, including, one would expect, security vulnerabilities which are a common problem in trying to make information systems more secure.

Section 816 encourages the establishment of additional computer forensic laboratories. In addition to assisting federal authorities to investigate and prosecute computer crimes, the laboratories are to train federal, state and local officials in computer forensics, to assist state and local officials in investigating and prosecuting state and local computer offenses, and to share expertise and information on the latest developments in computer forensics.

Electronic Communication Laws

The laws, which govern e-mail and keystroke interception, retrieval, and disclosure are known as the "electronic communications" laws. The most significant of these are the Electronic Communications Privacy Act, and portions of the USA PATRIOT Act. The following sections cover the specific aspects of these laws that information security professionals need to be aware of.

The Electronic Communications Privacy Act

Federal statutes protect electronic communications, including e-mail, instant messaging, and the keystrokes of network users (and sometime abusers) both from interception while they are being sent, and from access after they arrive at their destination. The Electronic Communications Privacy Act (ECPA) and its associated federal statutes prohibit the unauthorized interception or disclosure of such communications, but the level of protection for the communications differs depending upon whether the communications are in transit or are stored. Understanding how these laws work is also useful in understanding when your organization is the victim of a crime. More importantly, however, because the monitoring of electronic communications is an integral part of what information security professionals are asked to do, they should have a firm grasp of when such monitoring is authorized.

Electronic Eavesdropping or Real-Time Interception The real-time acquisition of electronic communications *in transit* is governed by the wiretap provisions of the ECPA, codified at 18 U.S.C. Section 2511 and following. Specifically, Section 2511(a) prohibits intentionally *intercepting* (or "endeavoring to intercept") any electronic communication, intentionally *disclosing* (or "endeavoring to disclose") the contents of any electronic communication knowing or having reason to know that the information was obtained through an illegal wiretap, or *using* (or "endeavoring to use") the information knowing it was obtained via an unlawful interception.[8] Practically speaking, the wiretap provisions make unlawful the use of packet sniffers or other devices designed to record the keystrokes of persons sending electronic communications, unless a legally recognized exception applies to authorize the conduct.

Naturally, information security professionals must be able to use electronic monitoring tools in maintaining and protecting their network environments. The wiretapping provisions of the ECPA recognize this reality and afford two primary exceptions (other than specific Title III wiretapping authorities for law enforcement) under which the interception of electronic communications is permitted: self-defense and consent. The self-defense or system provider exception states that a "provider of … electronic communication service" may intercept communications on its own machines "in the normal course of employment while engaged in any activity which is a necessary incident to … the protection of the rights or property of the provider of that service."[9]

The courts have not had occasion to define the contours of when such an activity is "necessarily incident" to protecting rights and property. What is certain, however, is that there must be some limitation on permissible monitoring, or the exception would swallow

[8] 18 U.S.C. § 2511(1)(a), (c), and (d).
[9] 18 U.S.C. § 2511(2)(a)(i).

the general prohibition. Whereas a system administrator's monitoring the keystrokes of an attacker who has gained access via a dormant account and attempted to elevate himself to root-level access surely falls squarely into the exception, periodic monitoring of the e-mail communications of all junior vice-presidents in a certain division of an organization seems to stretch beyond the rationale for the exception.

NOTE In some cases, an entity may monitor an attacker's activities for a period of time and then turn over the results of its own investigation to law enforcement. Once a criminal investigation related to the activity commences, it is unlawful for any person to disclose the communications obtained lawfully under the self-defense exception if done with the intent to impede or obstruct the criminal investigation, or if the communications were intercepted in connection with that criminal investigation.

The uncertainty of the self-defense exception's reach suggests that reliance on the second exception, *consent*, provides a far sounder footing in most instances. The Wiretap Act recognizes that it shall not be unlawful for a person to intercept an electronic communication where the person "is a party to the communication or where one of the parties to the communication has given prior consent to such interception."[10] The clearest form of consent is when an actual party to the communication seeks to record it. Under federal law, both parties need not consent to the recording or disclosure of e-mails or instant messages by either the sender or recipient of those messages. (Some states, however, require that *both* parties to a communication consent before the contents may be recorded or disclosed.)

In most instances where an organization calls upon its information security staff to monitor communications, however, the staff are not participants in the subject communications. The entity that owns the network is not automatically a party to an e-mail exchange between someone using its system and a third party outside the network. Accordingly, if that entity wishes to preserve the right to monitor such communications, it must ensure that it has previously obtained the consent to do so from all users of its network. The cleanest manner of ensuring consent to record all communications on an entity's network is to use a click-through banner as part of the login process, requiring any user of the system to accept that use of the system constitutes consent to the monitoring of all use of that network.

In the absence of such a banner, consent via organizational acceptable use policies and employee handbooks may suffice. When relying on consent obtained via policy or handbook, entities should be mindful of defining the consent broadly. Broad consents are increasingly necessary, due both to the proliferation of devices enabling the exchange of electronic communications (such as cell phones, smartphones, tablets, portable computing devices, and remote access programs), and to recent court cases extending the application of the wiretap provisions to activities that may be routinely monitored by organizations without regard to wiretapping concerns, such as tracking URLs visited by network users.[11]

[10] 18 U.S.C. § 2511(2)(d). The consent section does not apply, however, where the communication is intercepted for the purpose of committing any criminal or tortious act.

[11] *In re Pharmatrak Privacy Litigation*, 329 F.3d 9 (1st Cir. 2003).

Like the CFAA, the wiretap provisions of the ECPA permit civil suits to be brought for violations of the Act. Any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of the Act may recover actual, statutory, and/or punitive damages from the person or entity engaging in the offense.[12] Thus, criminal liability aside, it is critical that information security professionals are mindful about the types of interceptions they and their companies perform.

Stored Communications

Stored electronic communications, such as e-mail residing on a mail server, are protected by the stored communications provisions of the ECPA, codified at 18 U.S.C. Section 2701 and following. Specifically, Section 2701(a)(1) and (2) prohibit intentionally accessing, without or in excess of authorization, the facilities of a provider of electronic communications (an entity that provides users the ability to send and receive e-mail, not merely an individual's PC) and thereby obtaining, altering, or preventing authorized access to the electronic communications stored there.[13] Thus, hacking into an e-mail server for the purpose of obtaining access to stored e-mail is prohibited by the stored communications provisions. This prohibition applies equally to hacking into the e-mail servers of providers to the public (such as ISPs) and private providers of restricted networks belonging to organizations. In connection with the passage of the Homeland Security Act in 2002, violations where the offense is committed for purposes of commercial advantage or gain, malicious destruction, or in furtherance of another criminal or tortious act were elevated to a felony.

Significantly, unlike real-time interceptions, which are unlawful without an explicit exception, the review or recording of stored communications is lawful unless coupled with an unauthorized access to the information. For system administrators with root level access to their organization's e-mail servers, accessing these communications for legitimate purposes (doing so on behalf of the organization in a manner consistent with the organization's policies)

When Are Communications "Stored"?

Because the prohibitions on monitoring and accessing electronic communications differ significantly depending on whether the communications are characterized as "in transit" or "stored," this characterization is important. A case in which this became a deciding factor was *United States v Councilman*, 245 F.Supp.2d 319,321 (D. Mass. 2003), in which the First Circuit Court of Appeals dismissed charges of illegal wiretapping when the defendant intercepted a competitor's emails, claiming that communications held briefly in a system's RAM, or stored for a nanosecond while being routed across the Internet, are considered stored, and therefore the defendant was not "intercepting" communications. This decision was reversed in 2005, when the First Circuit's new decision was that even though emails are "stored" in memory during transit, it is still illegal to secretly intercept them. Subsequently in 2007, the defendant was acquitted, but the First Circuit's decision on the meaning of "stored" still stands.

[12] 18 U.S.C. § 2520(b) and (c).
[13] 18 U.S.C. § 2701.

will seldom, if ever, be unauthorized. Reviewing the system logs for non-content, transactional information is even less problematic. Of course, the technical ability to access e-mail is not coextensive with the level of authority to do so.

NOTE For example, a rogue system administrator who peruses an officer of the company's e-mail out of curiosity is likely violating company policy, and is potentially violating the ECPA by extension.

USA PATRIOT Act (Sections 105, 202, 210, 216, 220)

Section 105 provides certain powers to the U.S. Secret Service's Electronic Crime Task Force for investigating electronic crimes, for example "cloning" cell phones and denial-of-service attacks against on-line services. This section directs the Director of the Secret Service to develop a national network of computer security task forces from both government and private sectors.

Section 202 and Section 217 allow law enforcement officials to intercept electronic communications of "computer trespassers" if they have been given legal permission by the Attorney General, or other designated officials, via a court order to intercept targeted communications. A "computer trespasser" is defined as someone "who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication to, through, or from the protected computer" as long as the owner or operator of the protected computer authorizes the interception; the person acting under color of law is lawfully engaged in an investigation; the person acting under color of law has reasonable grounds to expect the content of the computer trespasser's communication is relevant to the investigation; and the interception acquires only the trespasser's communications within the invaded computer.

Section 210 expands the information that law enforcement officials may obtain (with appropriate authorization) from providers of electronic communications service or remote computing services regarding a subscriber or customer of those services to include a subscriber's or customer's means and source of payment, as well as allowing the collection of session times and network addresses, to improve the ability of law enforcement officials to track the activity and identity of suspects concerning a wide range of offenses, including terrorist activities and those of computer trespassers.

Section 216 allows authorities to use pen registers and trap and trace devices with a single court order and apply those devices to any computer or facility anywhere in the country. (Previously, authorization had to be obtained in each jurisdiction where the devices needed to be applied, and this was considered only to be relevant to telephony devices and not computers.)

Section 220 allows a single court with jurisdiction over the offense under investigation to issue a warrant allowing the search of electronic evidence anywhere in the country, whereas previously the warrant needed to be issued by a court within the jurisdiction where the information resided.

Other Substantive Laws

Other "substantive" laws, which address unlawful conduct either committed in cyberspace or assisted by computers, are described in the following sections.

Other Cyber Crimes

While the core cyber crimes are covered under the CFAA and ECPA, there are additional substantive provisions of criminal and civil law that may affect information security professionals in the course of their regular duties, and they should have some understanding of these laws. Each of the offenses discussed in this section are routinely encountered within organizations, and they generally involve the use of the organization's computer network to some degree. In many cases, the information security manager will be the first person in the organization to become aware of such activity, and he or she should have some basis for evaluating its significance. These offenses include theft of trade secrets, copyright and trademark infringement, and possession of child pornography. Each of the statutes governing this conduct is particularly relevant not only to causes of action against attackers and outsiders, but also to internal investigations.

Criminal theft of trade secrets is punishable under the Economic Espionage Act, codified at 18 U.S.C. Sections 1831–39. A defendant is guilty of economic espionage if, for economic benefit, she steals, or obtains without authorization, proprietary trade secrets related to a product involved in interstate commerce, with the knowledge or intent that the owner of the secret would suffer injury. This statute applies equally to trade secrets stolen by outsiders and those obtained without approval or authorization by employees. Civil cases of trade-secret theft must be filed under state trade-secret law.

Another discomforting problem for network administrators is the discovery of electronic contraband stored on their organization's network, whether placed there by an attacker or by an internal network user. Two pervasive examples of this issue are intellectual property infringement and child pornography. Intentional electronic reproduction of copyrighted works with a retail value of more than $2,500 is punishable by fine, imprisonment, or both via 18 U.S.C. Section 2319, Criminal Infringement of a Copyright. While this statute can apply to outsiders who copy an organization's products, it also applies to employees of an organization who host infringing content on the organization's network. (Criminal trademark infringement—for instance, selling pirated copies of software or musical works with a counterfeited mark—is likewise punishable by fine, imprisonment, or both via 18 U.S.C. Section 2320.) Increasingly, content owners are also targeting private organizations where they identify users of those networks who are actively engaging in the swapping of copyrighted materials via the organization's network. In such instances, the organization will generally not be held liable for the rogue actions of employees, particularly where they violate the organization's written policies. To ensure that the organization does not risk exposure, however, it is important to respond swiftly upon discovering infringing materials on the network.

18 U.S.C. Section 2252 and 18 U.S.C. Section 2252A prohibit the "knowing" possession of any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed or transported interstate by any means, including by computer. Actual knowledge or reckless disregard of the minority of the performers and of the sexually explicit nature of the material is required. Although there is some authority intimating that the intent requirement is satisfied when a defendant is aware of the nature of the material, the requirement that possession of such material is "knowing" was created specifically to protect people who have received child pornography by mistake. Therefore, individuals who unknowingly possess material meant for another are not implicated by the statute.

However, cases interpreting the federal statute have found that a party may be found to "knowingly" possess child pornography if it possesses such material for a long period of time and does not delete it. Accordingly, it is imperative that an entity take action upon attaining a sufficient level of knowledge that it is in possession of the contraband material. In many cases, an information security manager may discover an employee directory with a number of JPEG files with filenames suggestive of child pornography. If these images are not actually viewed, however, the requisite level of "knowledge" may not have crystallized, despite suggestive names. Courts have stated that filenames are not necessarily a reliable indicator of the actual content of files, and that it is rarely, if ever, possible to know if data in a file contains child pornography without viewing the file on a monitor.[14] Section 2252A(d) contains an affirmative defense to possession charges for anyone who promptly takes reasonable steps to destroy the images or report them to law enforcement, provided the person is in possession of three or fewer images. Although the defense is limited to three or fewer images, as a practical matter, if an employee is storing child pornography on an organization's network in violation of the organization's acceptable use policies, that conduct (even where the number of images far exceeds three) will not be imputed to the organization if it promptly takes action to delete the images or report them to the authorities.

State Legislation

A particularly useful resource for finding out what legislation has been proposed, and the status of each, is the National Conference of State Legislatures, which can be found at www.ncsl.org/default.aspx?tabid=13489. According to the NCSL Security Breach Legislation 2011 year-end summary (December 20, 2011):

> Information security experts are calling 2011 one of the worst years for data security breaches in the last 10 years. Since 2002, forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. In 2011, at least 14 states introduced legislation expanding the scope of laws, setting additional requirements related to notification, or changing penalties for those responsible for breaches.

Following are examples of state legislation that has passed, as summarized by NCSL in its 2011 year-end summary:

- **California, S.B. 24, Status: August 31, 2011; Signed by Governor** Requires any agency, person, or business that is required to issue a security breach notification pursuant to existing law to fulfill additional requirements pertaining to the security breach notification by electronically submitting a single sample copy of that security breach notification to the Attorney General. Provides that a covered entity under the federal Health Insurance Portability and Accountability Act is deemed to have complied with these provisions if it has complied with existing federal law.

NOTE What is new for California is the requirement to submit a sample copy of the breach notification to the Attorney General. California has had security breach notification law since SB1386, passed in 2003.

[14] *U.S. v Gray*, 78 F.Supp.2d 524, 529 (E.D. Va. 1999).

- **Illinois, H.B. 3025, Status: August 22, 2011; Public Act No. 483** Amends the Personal Information Protection Act; relates to security breaches; requires that certain information be provided in a disclosure notification to a State resident after a breach; provides for a delay of notification to prevent interference with a criminal investigation; provides that civil penalties may be imposed on certain contracted third parties; specifies that a person disposing of materials containing personal information must do so in a manner that renders the information undecipherable.

NOTE What is interesting about this piece of legislation is that it provides for a delay in notification to allow criminal investigation to occur and it addresses the disposal of materials containing personal information.

- **Nevada, S.B. 82, Status: June 13, 2011; Signed by Governor, Chapter 331** Relates to governmental information systems; requires the Chief of the Office of Information Security of the Department of Information Technology to investigate and resolve matters relating to security breaches of information systems of state agencies and elected officers; revises authority of the Department to provide services and equipment to local governmental agencies; authorizes the Chief of the Purchasing Division of the Department of Administration to publish advertisements for bids.
- **Nevada, S.B. 267, Status: June 13, 2011; Signed by Governor, Chapter 354** Revises provisions governing personal information and encryption. Prohibits a data collector from moving a data storage device which is used by or is a component of a multi-functional device beyond the control of the data collector, its data storage contractor or a person who assumes the obligation of the data collector to protect personal information unless the data collector uses encryption to ensure the security of the information. Provides for alternative methods or technologies to encrypt data.

The information security professional must keep abreast of individual state security legislation especially if the organization conducts business in numerous states.

Summary

The responsibilities of information security professionals continue to expand. In addition to keeping pace with the rapid advancements in security technology, these professionals increasingly must be aware of the emerging spate of information security laws and regulations. Enacting and administering effective information security policies and procedures requires that information security professionals understand the laws governing cyber crime, and these laws continue to evolve.

The most significant impact of legislation is that the "techies" are no longer solely responsible for defining "best practices" and "industry standards" for information security. Rather, defining and enforcing information security standards for consistency of practice across the United States is the province of Congress, state legislatures, and federal and state law enforcement agencies. In this regulated environment, information security professionals can expect to be working closely with counsel, outside auditors, and corporate boards to ensure that their organizations' information security practices not only protect the organization's network, but shield the organization from potential liability arising from cyber incidents.

References

Publications

Anand, Sanjay. *Sarbanes-Oxley Guide for Finance and Information Technology Professionals.* Wiley, 2006.

Beaver, Kevin, and Rebecca Herold. *The Practical Guide to HIPAA Privacy and Security Compliance.* 2nd ed. Auerbach, 2011.

Brand, Koen. *IT Governance based on COBIT 4.1 - A Management Guide.* 3rd ed. Van Haren Publishing, 2007.

Calder, Alan, and Steve Watkins. *IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002.* 4th ed. Kogan Page, 2008.

Dlamini, M., J. H. P. Eloff, and M. Eloff. "Information Security: The Moving Target." *Computers & Security* 28, issue 3–4 (2009): 189–198.

Easttom, Chuck, and Jeff Taylor. *Computer Crime, Investigation, and the Law.* Course Technology PTR, 2010.

Flick, Tony, and Justin Morehouse. *Securing the Smart Grid: Next Generation Power Grid Security.* Syngress, 2010.

Gilling, T. *Beginner's COBIT Companion.* Troubador Publishing Ltd, 2009.

Hartley, Carolyn P., and Edward D. Jones III. *HIPAA Plain & Simple: A Healthcare Professionals Guide to Achieve HIPAA and HITECH Compliance.* American Medical Association Press, 2010.

Hintzbergen, Jule, Kees Hintzbergen, Andre Smulders, and Hans Baars. *Foundations of Information Security Based on ISO27001 and ISO27002.* Van Haren, 2010.

IT Governance Institute. *COBIT Security Baseline: An Information Survival Kit.* 2nd ed. IT Governance Institute, 2007.

Knapp, Eric. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems.* Syngress, 2011.

Lahti, Christian, and Roderick Peterson. *Sarbanes-Oxley IT Compliance Using Open Source Tools.* Syngress, 2007.

Landy, Gene, and Amy Mastrobattista. *The IT/Digital Legal Companion: A Comprehensive Business Guide to Software, IT, Internet, Media and IP Law.* Syngress, 2008.

Nicholls, Kathy. *Stedman's Guide to the HIPAA Privacy & Security Rules.* 2nd ed. Lippincott Williams & Wilkins, 2011.

Reed, Chris, and John Angel. *Computer Law: The Law and Regulation of Information Technology.* Oxford University Press, 2007.

Reyes, Anthony, Richard Brittson, Kevin O'Shea, and James Steele. *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors*. Syngress, 2007.

Tatom, John. *Financial Market Regulation: Legislation and Implications*. Springer, 2011.

von Solms, S., and Rossouw von Solms. *Information Security Governance*. Springer, 2008.

Wu, Stephen. *A Guide to HIPAA Security and the Law*. American Bar Association, 2007.

Online Resources

COBIT resources: www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx

ISO 27002 official page: www.iso.org/iso/catalogue_detail?csnumber=50297

NIST Special Publications (800 Series): csrc.nist.gov/publications/PubsSPs.html

CRS Report for Congress: epic.org/privacy/terrorism/usapatriot/RL31289.pdf